DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) 22 September 2017

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the NetApp, Inc. Fabric Attached Storage (FAS)/All Flash FAS (AFF) Data Storage Controllers (DSCs) on ONTAP Release 9.1

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013, Change 1," June 2016
(c) through (d), see Enclosure

1. **Certification Authority.** Reference establish the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for the Department of Defense Information Network (DoDIN) products, Reference (b).

2. **Conditions of Certification.** The NetApp, Inc. FAS/AFF DSCs on ONTAP Release 9.1; hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements (UCR), Reference (b), and is certified for joint use as a Data Storage Controller (DSC) with the conditions described in Table 1. The FAS8040 was the model tested; however, the models listed in Table 4 utilize the same software and similar hardware. JITC analyses determined these systems to be functionally identical to the FAS8040 and therefore, they are covered under this certification. This certification expires upon changes that affect interoperability, but no later than the expiration date listed in the DoDIN Approved Products List (APL) memorandum.

**Table 1. Conditions**

| Condition | Operational Impact | Remarks |
|---|---|---|
| **UCR Waivers** | | |
| None. | | |
| **Conditions of Fielding** | | |
| **TDR NAI-0648-001**: The SUT does not Support the GNS or single Name space functionality. The SUT supports only "in-band" (local) single namespace functionality. Not certified for "out-of-band" Global Namespace support. | Minor | See note 1. |
| **Open Test Discrepancies** | | |
| **TDR NAI-0648-002**: The SUT did not support the 1 Gigabit Ethernet (GbE) for Network Attached Storage. | None | See note 2. |
| **TDR NAI-0648-003**: Per the vendor LoC, the SUT does not support Redirect requirements for IP6-000350. | Minor | See note 3. |

**Table 1. Conditions (continued)**

| Condition | Operational Impact | Remarks |
|---|---|---|
| **Open Test Discrepancies (continued)** | | |
| **TDR NAI-0648-004**: The SUT did not support Fiber Channel (FC) zones. | None | See note 2. |

**NOTES:**
1. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact with a condition of fielding. The SUT does not support disparate and remote network based file systems because the GNS exists within a DSC cluster which must be co-located in a campus type environment. The SUT supports only "in-band" (local) single namespace functionality. The SUT is not certified for "out-of-band" Global Namespace support.
2. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as a change requirement and having a no operational impact. DISA stated the intent to change this requirement in the next version of the UCR.
3. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact.

**LEGEND:**

| | | | |
|---|---|---|---|
| DISA | Defense Information Systems Agency | LoC | Letter of Compliance |
| DSC | Data Storage Controller | POA&M | Plan of Action and Milestones |
| GbE | Gigabit Ethernet | RFC | Requests for Comment |
| GNS | Global Name Service | SUT | System Under Test |
| FC | Fiber Channel | UCR | Unified Capabilities Requirements |
| IPv6 | Internet Protocol Version 6 | | |

3. **Interoperability Status.** Table 2 provides the SUT interface interoperability status and Table 3 provides the Capability Requirements (CR) and Functional Requirements (FR) status. Table 4 provides a DoDIN APL product summary.

**Table 2. SUT Interface Status**

| Interface | Threshold CR/FR Requirements (See Note 1.) | Status | Remarks |
|---|---|---|---|
| **Network Attached Storage (NAS) Interfaces** | | | |
| 1 GbE (Ethernet) (R) | 1 | Not Met | See Note 2. |
| 10 GbE (Ethernet) (R) | 1 | Met | |
| **Storage Array Net (SAN) Interfaces** | | | |
| Fibre Channel (FC) | 1 | Met | |
| FC Protocol (FCP) | 1 | Met | |
| **Out-of-band Management Interfaces** | | | |
| 10 Mbps Ethernet (R) | 1 | Met | |
| 100 Mbps Ethernet (R) | 1 | Met | |
| 1 GbE Ethernet (R) | 1 | Met | |
| **Converged Network Adapter (CNA) Interfaces** | | | |
| 10 GbE (Ethernet) (R) | 1 | Met | |

**NOTE(S):**
1. The UCR does not identify interface CR/FR applicability. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column are cross-referenced with Table 3.
2. The SUT does not support 1 GbE NAS interfaces. DISA adjudicated this discrepancy as a change requirement with no operational impact.

**LEGEND:**

| | | | |
|---|---|---|---|
| CNA | Converged Network Adapter | NAS | Network Attached Storage |
| CR | Capability Requirement | R | Required |
| FR | Functional Requirement | SAN | Storage Array Net |
| GbE | Gigabit Ethernet | SUT | System Under Test |
| ID | Identification | UCR | Unified Capabilities Requirements |
| Mbps | Megabits per second | | |

### Table 3. SUT Capability Requirements and Functional Requirements Status

| CR/FR ID | UCR Requirement (High-Level) (See note 1.) | UCR 2013 Reference | Status |
|---|---|---|---|
| 1 | Data Storage Controller (DSC) (R) | Section 14 | Partially Met (See notes 2 and 3.) |

**NOTES:**
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.
2. The SUT met the requirements with the exceptions noted in Table 1. DISA adjudicated these exceptions as minor or as change requirements.
3. Security testing was accomplished by JITC-led Cybersecurity test teams and the results published in a separate report, Reference (e).

**LEGEND:**

| | | | |
|---|---|---|---|
| CR | Capability Requirement | R | Required |
| DISA | Defense Information Systems Agency | SUT | System Under Test |
| FR | Functional Requirement | UCR | Unified Capabilities Requirements |
| ID | Identification | | |

### Table 4. DoDIN APL Product Summary

| | | | |
|---|---|---|---|
| **Product Identification** | | | |
| Product Name | NetApp, Inc. FAS / AFF DSCs on ONTAP | | |
| Software Release | ONTAP 9.1 | | |
| DoDIN Product Type(s) | Data Storage Controller | | |
| Product Description | The SUT performs data replication, mirroring, back-up, continuance of operation, and disaster recovery functions. | | |
| **Product Components (See note 1.)** | **Component Name (See note 2.)** | **Version** | **Remarks** |
| Primary and Secondary Data Storage Controller (x2) | **FAS8040,** FAS2520, FAS2552, FAS2554, FAS2620 AFF A200, FAS2650, FAS8020, FAS8040, AFF8040, FAS8200, AFF A300, FAS8060, FAS8080 EX, AFF8080 EX, FAS9000, AFF 700, AFF A700s | 9.1 | See note 3. |

**NOTES:**
1. The detailed component and subcomponent list is provided in Enclosure 3.
2. Components bolded and underlined were tested by JITC. The other components in the family series were not tested, but are also certified for joint use. JITC certifies those additional components because they utilize the same software and similar hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes.
3. Expanded I/O products have a dual enclosure and 12 PCIe expansion slots instead of a single enclosure and 4 PCIe expansion slots.

**LEGEND:**

| | | | |
|---|---|---|---|
| AFF | All Flash FAS | IOXM | I/O Expansion Module |
| APL | Approved Products List | JITC | Joint Interoperability Test Command |
| DSCs | Data Storage Controllers | PCIe | Peripheral Component Interconnect Express |
| FAS | Fabric Attached Storage | SUT | System Under Test |
| I/O | Input/Output | UC | Unified Capabilities |

4. **Test Details.** This certification is based on interoperability testing, review of the vendor's Letters of Compliance (LoC), DISA adjudication of open test discrepancy reports (TDRs), and DISA Certifying Authority (CA) Recommendation for inclusion on the DoDIN APL. Testing was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 5 through 16 June 2017 using test procedures derived from Reference (d). Review of the vendor's LoC was completed on 5 June 2017. DISA adjudication of TDRs was completed on 24 August 2017. Cybersecurity (CS) testing was conducted by JITC-led CS test teams and the results are published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

5. **Additional Information.** JITC distributes interoperability information via the JITC

Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified IP Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the Cybersecurity Assessment Package (CAP) that contains the approved configuration and deployment guide must be requested directly from the APCO, e-mail: disa.meade.ie.list.approved-products-certification-office@mail.mil. All associated information is available on the DISA APCO website located at http://www.disa.mil/Services/Network-Services/UCCO.

6. **Point of Contact (POC). Point of Contact (POC).** The JITC point of contact is Ms. Sibylle Gonzales, commercial telephone (520) 538-5483, DSN telephone 879-5483, FAX DSN 879-4347; e-mail address Sibylle.j.gonzales.civ@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTE (Ms. Sibylle Gonzales) P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The APCO tracking number for the SUT is 1629202.

FOR THE COMMANDER:

CLARK.BRADLEY.ALAN.
1231466564

Digitally signed by CLARK.BRADLEY.ALAN.1231466564
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA,
cn=CLARK.BRADLEY.ALAN.1231466564
Date: 2017.10.04 12:50:36 -07'00'

3 Enclosures a/s

for RIC HARRISON
Chief
Networks/Communications and UC Division

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS USD(AT&L)
ISG Secretariat, DISA, JTA
U.S. Strategic Command, J665 US
Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ
US Air Force, A3CNN/A6CNN
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division US
Coast Guard, CG-64
DISA/TEMC
DIA, Office of the Acquisition Executive NSG
Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS IV&V HQUSAISEC,
AMSEL-IE-IS
APCO

## ADDITIONAL REFERENCES

(c) Joint Interoperability Test Command, “Data Storage Controller (DSC) Test Procedures For Unified Capabilities Requirements (UCR) 2013 Change 1,” August 2016
(d) Joint Interoperability Test Command, “Cybersecurity Assessment Report for NetApp, Inc. Fabric Attached Storage (FAS)/All Flash FAS (AFF) Data Storage Controllers (DSCs) on ONTAP Release 9.1 (Tracking Number 1629202),” June 2017

## CERTIFICATION SUMMARY

**1. SYSTEM AND REQUIREMENTS IDENTIFICATION.** The NetApp, Inc. Fabric Attached Storage (FAS)/All Flash FAS (AFF) Data Storage Controllers (DSCs) on ONTAP Release 9.1 is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

**Table 2-1. System and Requirements Identification**

| | |
|---|---|
| **System Identification** | |
| Sponsor | United States Army |
| Sponsor Point of Contact | Jordan Silk, jordan.r.silk.civ@mail.mil, 520-533-7218 |
| Vendor Point of Contact | Michael Scanlin, Michael.Scanlin@netapp.com, 919-476-8578 |
| System Name | NetApp FAS/AFF DSCs on ONTAP |
| Increment and/or Version | 9.1 |
| Product Category | Data Storage Controller |
| **System Background** | |
| Previous certifications | Data ONTAP - 7-Mode 8.2.1 (TN 1324201)<br>Data ONTAP - Cluster Mode 8.2.1 (TN 1324202) |
| **Tracking** | |
| APCO ID | 1629202 |
| System Tracking Program ID | 4544 |
| **Requirements Source** | |
| Unified Capabilities Requirements | Unified Capabilities Requirements 2013, Change 1 |
| Remarks | |
| **Test Organization(s)** | Joint Interoperability Test Command, Fort Huachuca, Arizona |

**LEGEND:**

| | | | |
|---|---|---|---|
| AFF | All Flash FAS | ID | Identification |
| APCO | Approved Products Certification Office | JITC | Joint Interoperability Test Command |
| DoDIN | Department of Defense Information Network | TN | Tracking Number |

**2. SYSTEM DESCRIPTION.** A Data Storage Controller (DSC) is a specialized multiprotocol computer system with an attached disk array that serves in the role of a disk array controller and end node in Base/Post/Camp/Station (B/P/C/S) networks. The DSC is typically a Military Department (MILDEP) asset connected to the Assured Services Local Area Network (ASLAN); however, the DSC is not considered part of the ASLAN.

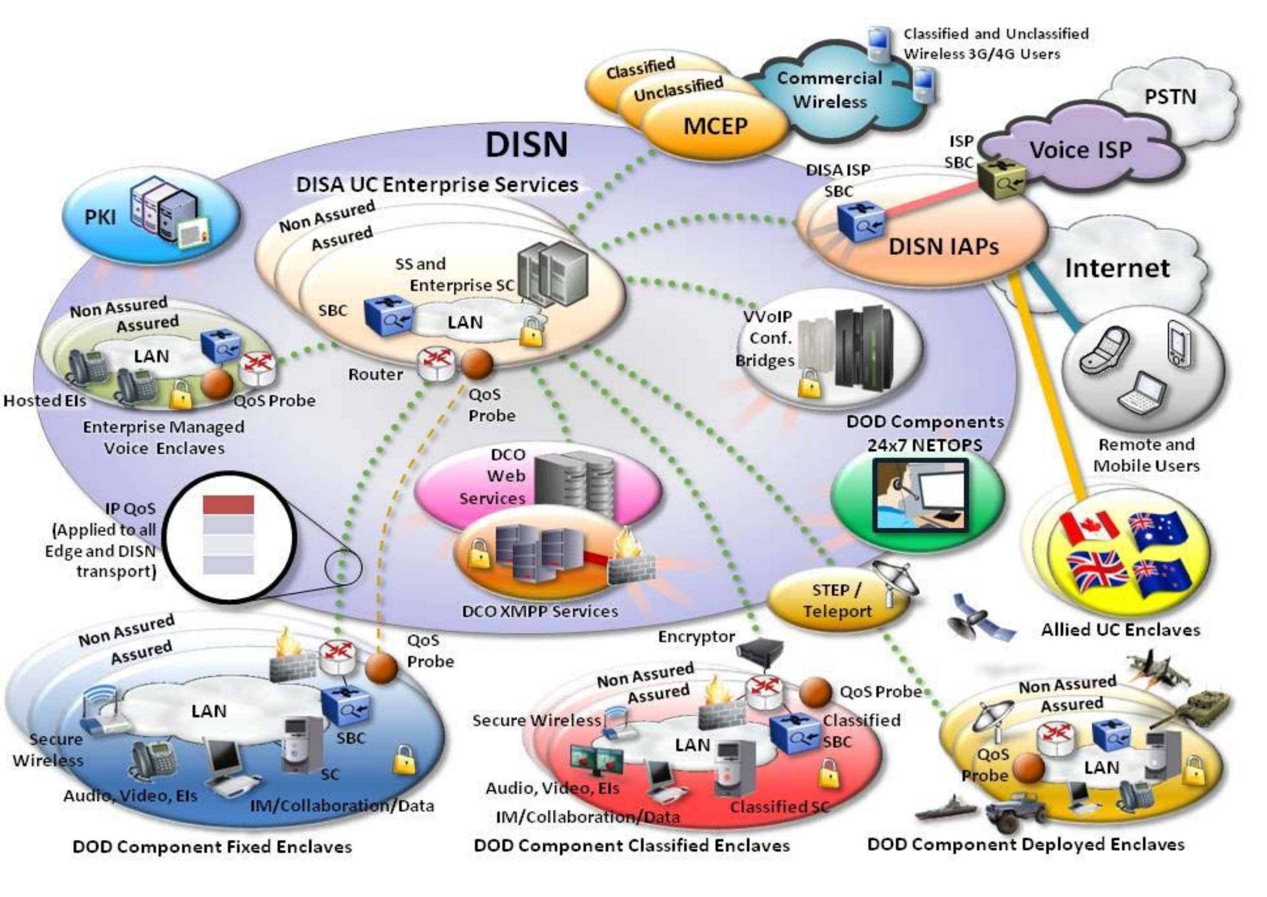
**a. General Description**. The SUT is a cross-platform hardware- and software-based data storage and retrieval system. The SUT responds to network requests from clients and fulfills them by writing data to or retrieving data from the disk arrays. The SUT provides a modular hardware architecture running the Data ONTAP operating system and WAFL (Write Anywhere File Layout) software. Data ONTAP is the operating system for all NetApp storage systems. The SUT provides a complete set of storage management tools through a command-line interface, through System Manager and FilerView, through the DataFabric Manager (which requires a license), and through the remote management device such as the Service Processor (SP), the Remote Local Area Network (LAN) Module (RLM), or the Baseboard Management Controller (BMC) form data storage system.

**b. Management Description.** The SUT is managed with a site-provided, Security Technical Implementation Guide (STIG)-compliant, Common Access Card (CAC)-enabled workstation.

**3. OPERATIONAL ARCHITECTURE.** The Department of Defense Information Network (DoDIN) architecture is a two- level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The Department of Defense (DoD) Chief Information Officer (CIO) and Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The UC architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational DoDIN architecture in which the SUT may be used and Figure 2-2 the DSC functional model.

**4. TEST CONFIGURATION.** The test team tested the SUT at JITC, Fort Huachuca, Arizona in a manner and configuration similar to that of a notional operational environment. Testing of the system's required functions and features was conducted using the test configurations depicted in Figures 2-3. Information Assurance testing used the same configurations.

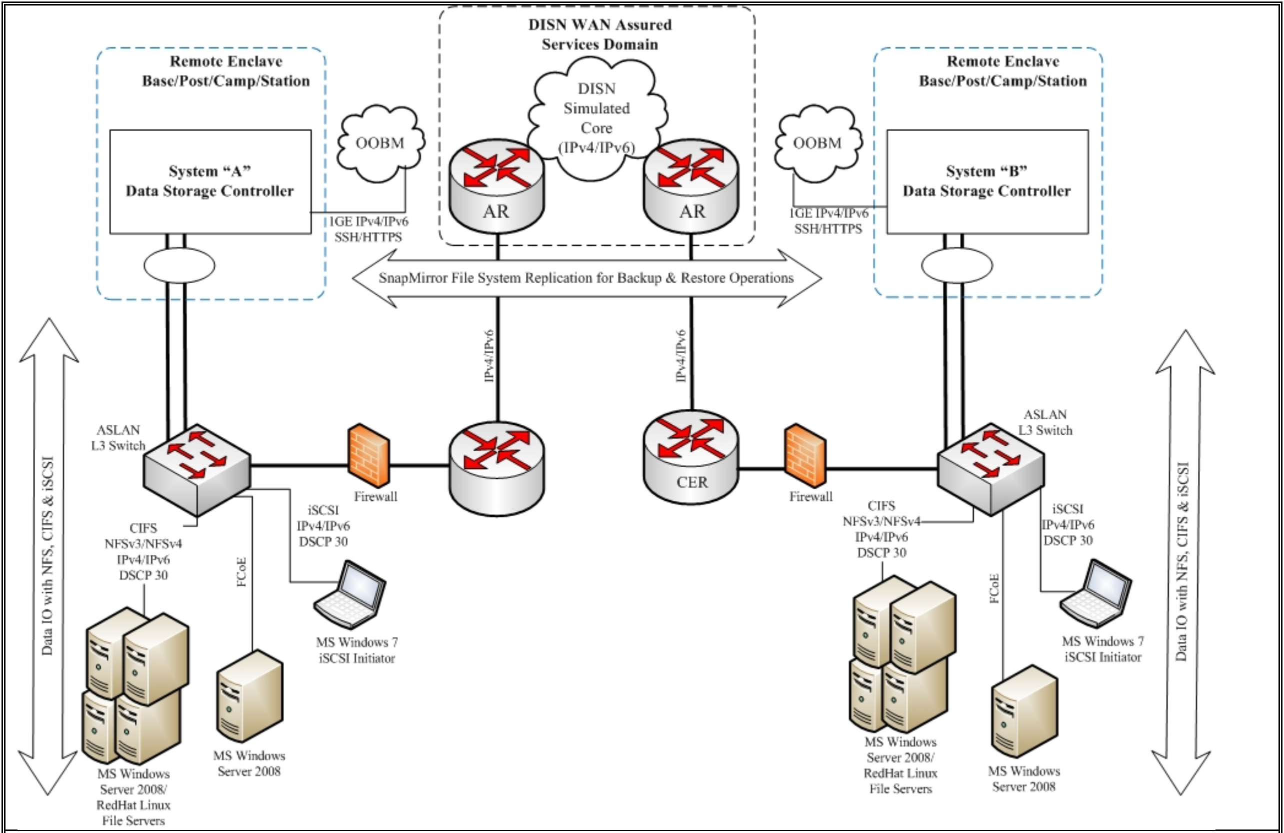
**5. METHODOLOGY.** Testing was conducted using DSC requirements derived from the Unified Capabilities Requirements (UCR) 2013, Reference (c), and DSC test procedures, Reference (d). Any discrepancies noted were written up in Test Discrepancy Reports (TDRs). The vendor submitted Plan of Action and Milestones (POA&M) as required. The remaining open TDRs were adjudicated by Defense Information Systems Agency (DISA) as minor. Any new discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor POA&M, which will address all new critical TDRs within 120 days of identification.



**LEGEND:**

| | | | |
|---|---|---|---|
| DCO | Defense Connection Online | NETOPS | Network Operations |
| DISA | Defense Information Systems Agency | PKI | Public Key Infrastructure |
| DISN | Defense Information Systems Network | PSTN | Public Switched Telephone Network |
| DoD | Department of Defense | QoS | Quality of Service |
| EI | End Instrument | SBC | Session Border Controller |
| IAP | Internet Access Point | SC | Session Controller |
| IM | Instant Messaging | SS | Softswitch |
| IP | Internet Protocol | STEP | Standardized Tactical Entry Point |
| ISP | Internet Service Provider | UC | Unified Capabilities |
| LAN | Local Area Network | VVoIP | Voice and Video over IP |
| MCEP | Multi Carrier Entry Point | XMPP | Extensible Messaging and Presence Protocol |

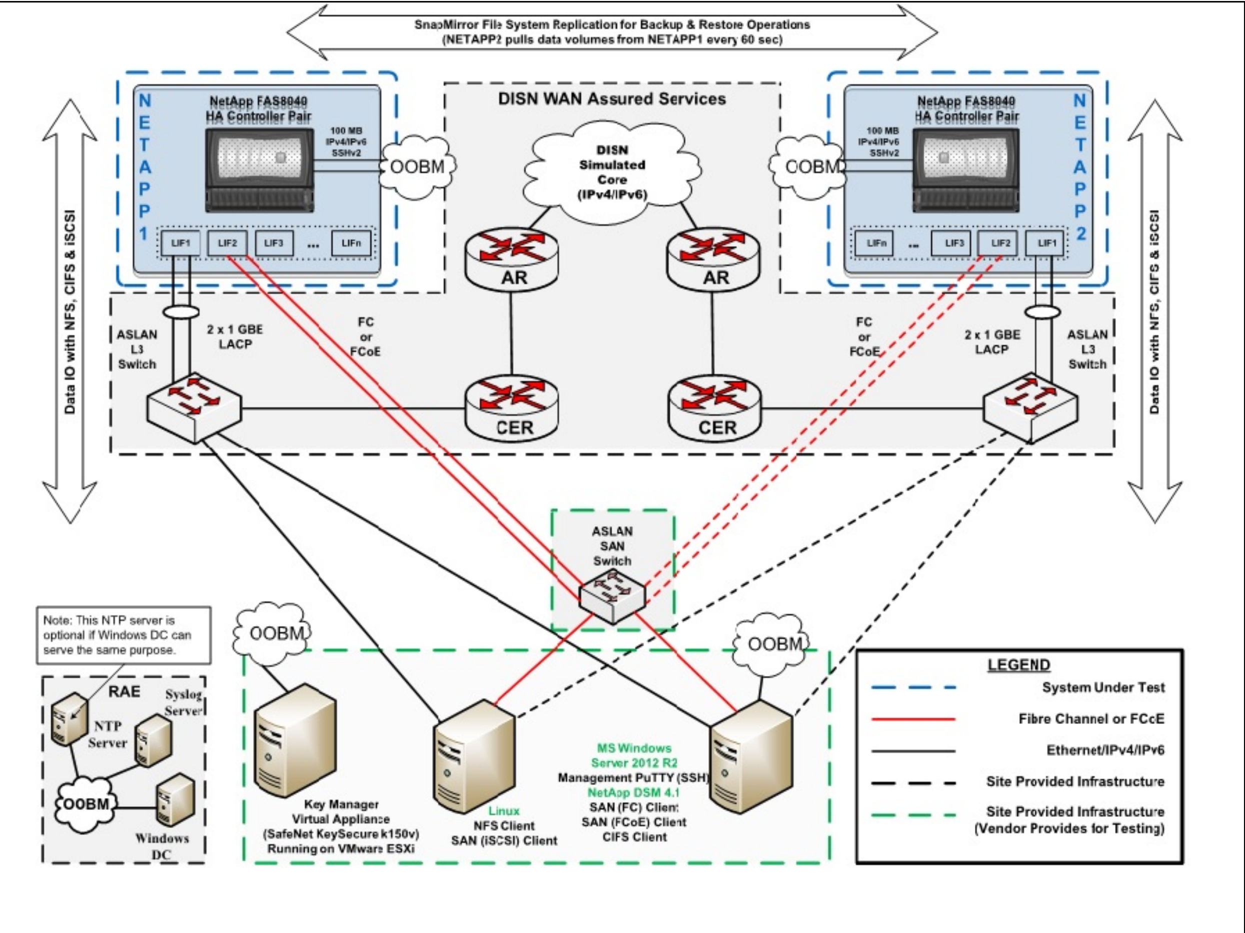
**Figure 2-1. Notional DoDIN Network Architecture**


DISN WAN Assured Services Domain
DISN Simulated Core (IPv4/IPv6)
AR
AR
Remote Enclave Base/Post/Camp/Station
System "A" Data Storage Controller
OOBM
1GE IPv4/IPv6 SSH/HTTPS
Remote Enclave Base/Post/Camp/Station
System "B" Data Storage Controller
OOBM
1GE IPv4/IPv6 SSH/HTTPS
SnapMirror File System Replication for Backup & Restore Operations
IPv4/IPv6
IPv4/IPv6
Data IO with NFS, CIFS & iSCSI
ASLAN L3 Switch
Firewall
CER
Firewall
ASLAN L3 Switch
Data IO with NFS, CIFS & iSCSI
CIFS NFSv3/NFSv4 IPv4/IPv6 DSCP 30
FCoE
iSCSI IPv4/IPv6 DSCP 30
MS Windows 7 iSCSI Initiator
MS Windows Server 2008/ RedHat Linux File Servers
MS Windows Server 2008
CIFS NFSv3/NFSv4 IPv4/IPv6 DSCP 30
FCoE
iSCSI IPv4/IPv6 DSCP 30
MS Windows 7 iSCSI Initiator
MS Windows Server 2008/ RedHat Linux File Servers
MS Windows Server 2008

**LEGEND:**

| | |
|---|---|
| AR | Aggregation Router |
| ASLAN | Assured Services Local Area Network |
| CER | Customer Edge Router |
| CIFS | Common Internet File System |
| DISN | Defense Information Systems Network |
| DSCP | Differentiated Services Code Point |
| FCoE | Fibre Channel Over Ethernet |
| GE | Gigabit Ethernet |
| HTTPS | Hypertext Transfer Protocol |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| iSCSI | Internet Small Computer Systems Interface |
| L3 | Layer 3 |
| MS | Microsoft |
| NFSv3 | Network File System version 3 |
| NFSv4 | Network File System version 4 |
| OOBM | Out of Band Management |
| SSH | Secure Shell |
| WAN | Wide Area Network |

**Figure 2-2. Data Storage Controller Functional Reference Model**



**LEGEND:**

| | | | |
|---|---|---|---|
| AR | Access Router | IP | Internet Protocol |
| ASLAN | Assured Service Local Area Network | L | Layer |
| CER | Customer Edge Router | LACP | Link Aggregation Control Protocol |
| CIFS | Common Internet File System | LF | Line Feed |
| DISA | Defense Information System Agency | OOBM | Out of Band Management |
| FAS | Fabric Attached Storage | NFS | Network File System |
| FC | Fibre Channel | NTP | Network Time Protocol |
| FCoE | Fibre Channel over Ethernet | RAE | Required Ancillary Equipment |
| GBE | Gigabit Ethernet | SAN | Storage Area Network |
| IO | Input Output | WAN | Wide Area Network |
| iSCSI | Internet Small Computer System Interface | | |

**Figure 2-3. SUT Test Configuration**

**6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS.** The interface, Capability Requirements (CR) and Functional Requirements (FR), and other requirements for DSCs are established by UCR 2013, Errata 1, sections 14, 5, and 4.

**a. Interface Status.** The JITC testing interface status of the SUT is provided in Table 3-1. The DSC shall provide physical interfaces for, as a minimum, Gigiabit Ethernet (GbE) and 10 GbE in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet Local Area Network (LAN) interfaces. The SUT met the 1 GbE and 10 GbE Ethernet LAN interfaces requirements with testing. The system shall provide physical interfaces for out-of-band management (OOBM) access and services with 10/100 Megabit per second (Mbps) Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: Secure Shell version 2 (SSHv2), Transport Layer Security (TLS), Hyper Text Transfer Protocol Secure (HTTPS), and Simple Network Management Protocol (SNMP) version 3; and the protocols shall be secured in accordance with Section 4, Information Assurance. The SUT met this requirement with testing. The system may optionally provide Fiber Channel (FC) physical interfaces and FC Protocol (FCP) interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303. The SUT met this optional requirement with the testing. The system shall provide physical interfaces for FC over Ethernet (FCoE) services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA). The SUT met this requirement with testing.

**b. Capability and Functional Requirements and Status.**

(1) The UCR 2013, section 14.2 includes the Storage System requirements in the subparagraphs below.

(a) The system shall provide a Redundant Array of Independent Disks (RAID) for multiple disk drives. The system shall provide a configuration option to select the specific RAID level to be provisioned in the disk array. The RAID levels available for use shall be subject to the specific vendor implementation. At a minimum, the RAID level shall be dual parity RAID-6 for Serial Advanced Technology Attachment (SATA) drives and RAID-5 for Serial Attached Small Computer Systems Interface (SCSI) and FC drives, although stronger RAID levels are acceptable. The SUT utilizes dual parity Server Attached Storage (SAS) drives which are equivalent to dual parity RAID-6 drives. The SUT met this requirement with testing. Testing included removing two of the SAS drives while writing data to Common Internet File System (CIFS) share using the 10GbE interface. The degraded drive status were displayed in the system status.

(b) The system shall be capable of 99.9 percent availability. The SUT met this requirement with the vendor’s Letter of Compliance (LoC), redundant equipment including but not limited to power supplies, data storage controllers, dual parity SAS drives, and vendor product availability documentation.

(c) The system shall provide a management control function for low-level system monitoring and control functions, interface functions, and remote management. The management control function shall provide an Ethernet physical interface(s) for connection to the owner’s (i.e., MILDEP) management network/LAN and also provide status. The monitoring shall include an initial system check, system cooling fans, temperatures, power supplies, voltages, and system power state tracking and logging. The SUT met this requirement with testing. Testing included a powering off one of the two power supplies. The SUT displayed the correct status and continued working. The system health status was reviewed prior and after the power supply was powered off.

(d) The system shall provide data storage replication (e.g., mirroring) services [Internet protocol (IP) version 4 (IPv4) and version 6 (IPv6)] between systems that are configured as source and destination replication pairs. The replication operations shall provide capabilities for data backup replication, system replication and migration, and system disaster recovery (DR) services in support of continuity of operations (COOP) planning. The SUT met this requirement with testing. Testing included data backup, replication, system replication and migration, and data recovery operations.

(e) When the system interfaces to an Integrated Data Protection (IDP) service and the IDP makes copies of data storage information on to another DSC for periodic data storage backup, DR/COOP, migration, and data archiving operation, the system replication service shall complete the replication regardless of the host connection protocols used between the application servers and the DSC. The SUT met this requirement with the vendor LoC.

(f) The system replication and migration services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for migrating data storage information. The SUT met this requirement with testing. Data storage and configuration information was replicated onto a standby DSC using regular scheduled backup operation using asynchronous replication mode.

(g) The system DR services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for DR/COOP. The SUT met this requirement with testing. Testing included backing up and replicating data storage and configuration information onto a standby DSC. The data on the standby DSC was accessible for DR/COOP.

(h) The system shall provide configurable modes for replication (mirroring) operations between the source DSC and the destination DSC. During replication, both the source and the destination must be in a known good state. The configurable modes shall be Asynchronous or Synchronous and are depicted in UCR 2013, Change 1, Table 14.2-1, Replication Operation Modes. The SUT met this requirement with the Asynchronous mode only. Testing included replicating data utilizing incremental block based replication occurring once per minute and manually entering a command that triggered the replication.

(2) The UCR 2013, section 14.3 includes the Storage Protocol requirements in the subparagraphs below.

(a) The system shall provide a Network File System version 3 (NFSv3) server for file systems data input/output (I/O). The SUT met this requirement with tested using Red Hat Linux. The SUT currently does not support NFS for Windows and therefore NFS for Windows is not included in this certification.

(b) The system shall provide a NFS version 4 (NFSv4) server for file systems data I/O. This optional requirement was not tested and therefore is not included in this certification.

(c) The system shall provide a NFS version 4.1 (NFSv4.1) server, including support for parallel NFS for file systems data I/O. This optional requirement was not tested and therefore is not included in this certification.

(d) The system shall provide a CIFS version 1.0 (CIFSv1.0) server for file systems data I/O. The SUT does not support CIFSv1.0. CIFSv1.0 is no longer used due to associated security risks.

(e) The system shall provide a CIFS version 2.0 (CIFSv2.0) server for file systems data I/O. The SUT met this optional requirement with testing using a Windows based client. Wireshark captures showed protocol features.

(f) The system shall provide Internet Small Computer Systems Interface (iSCSI) server (target) operations for data I/O of Logical Units (LUNs) to clients (initiators). The SUT met this optional requirement with testing using a Windows based client. Testing included the creation of LUNs, copying data files from the client machine to one of the LUNs, editing and reading copied files.

(g) The system shall provide FCP server (target) operations for data I/O of FCP LUNs to clients (initiators). The SUT met this optional requirement with testing using a Windows based client. Testing included the creation of LUNs, copying data files from the client machine to one of the LUNs, editing and reading copied files using FCP only. All interfaces except the FCP interface were disconnected during the test.

(h) The system shall provide FCoE server (target) operations for data I/O of FCP LUNs to clients (initiators). The SUT met this optional requirement with testing using a Windows based client. Testing included the creation of LUNs, copying data files from the client machine to one of the LUNs, editing and reading copied files using FCoE only. All interfaces except the FCoE interface were disconnected during the test.

(i) The system shall provide a HTTPS server for file system data I/O and management access to the storage controller operating system. The session shall be secured with SSL or Transport Layer Security (TLS), per Internet Engineering Task Force (IETF) Request for Comment (RFC) 5246, and shall comply with Section 4, Information Assurance, for that protocol. Although the SUT supports HTTPS server file system Input/Output, this optional requirement was not tested and therefore is not included in this certification.

(j) The system shall provide SSHv2 or TLS for management access to the storage controller operating system. The SSHv2 or TLS implementation shall comply with Section 4, Information Assurance, for that protocol. The SUT met this requirement with testing. SSHv2 was used for management access to the storage controller operating system.

(k) The system shall provide Web-based Distributed Authoring and Versioning (WebDAV), per IETF RFC 4918, in support of Cloud-based virtualized storage infrastructures. The SUT does not support this optional requirement.

(l) The system shall implement the Representational State Transfer (REST) software architecture for distributed hypermedia systems and Cloud-based virtualized storage infrastructures. The SUT does not support this optional requirement.

(m) The system shall implement the Storage Networking Industry Association (SNIA) Cloud Data Management Interface (CDMI) standard. The SUT does not support this optional requirement.

(n) The system shall provide Global Name Space (GNS) or single name space functionality. The GNS functionality shall provide the capability to aggregate disparate and remote network-based file systems to provide a consolidated view to reduce complexities of localized file management and administration. The GNS functionality shall provide large (i.e., 14 Petabyte [PB] or greater) working pools of disks, transparent data migration, and it shall serve to reduce the number of storage mount points and shares. Each system shall have a dedicated and unique GNS. The SUT does not support disparate and remote network based file systems because the GNS exists within a DSC cluster which must be co-located in a campus type environment. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact with a condition of fielding. The SUT supports only "in-band" (local) single namespace functionality. The SUT is not certified for "out-of-band" Global Namespace support.

(3) The UCR 2013, section 14.4 includes the Network Attached Storage Interface requirements in the subparagraphs below.

(a) The system shall provide physical interfaces for Gigabit Ethernet (GbE) and 10 Gigabit Ethernet (10 GbE) services in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet LAN interfaces. The SUT met this requirement with testing for the 10 GbE interface. The SUT does not support 1 GbE Network Attached Storage Interfaces; the 1 GbE interfaces are not included in the certification. DISA adjudicated this discrepancy as a change requirement for the next release of the UCR. Wireshark captures showed no anomalies during the test with the 10 GbE interface.

(b) The system shall be able to provision, monitor, and detect faults, and to restore Ethernet services in an automated fashion. The SUT met this requirement with the vendor's LoC, system logs, and system monitoring tool.

(c) The system shall provide physical interfaces for OOBM access and services with 10/100 Mbps Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: SSHv2, SSL, HTTPS, and SNMPv3; and the protocols shall be secured in accordance with Section 4, Cybersecurity. The SUT met this requirement with testing the remote access using SSHv2. CS testing is accomplished by a JITC-led Cybersecurity test team and the results published in a separate report, Reference (e).

(d) When the system uses Ethernet, Fast Ethernet, GbE, and 10GbE interfaces, the interfaces shall be autosensing, auto-detecting, and auto-configuring with incoming and corresponding Ethernet link negotiation signals. Autosensing, auto-detecting, and auto-configuring only applies to interfaces below 10GbE interfaces. This requirement was met with the OOBM interfaces only since the NAS interfaces were above 1 GbE.

(e) Ethernet services of the system and the Logical Link Interworking Function (IWF) of the system shall terminate the Media Access Control (MAC) layer of Ethernet as described in Ethernet Standard IEEE 802.3. The SUT met this requirement with testing and the vendor's LoC.

(f) Ethernet services of the system shall support jumbo frames with a configurable Maximum Transmission Unit (MTU) of 9000 bytes or greater, excluding Ethernet encapsulation. When Ethernet encapsulation is included in the frame size calculation, an additional 22 bytes must be included for the MAC header (14 bytes), the Virtual LAN (VLAN) tag (4 bytes), and the Cyclical Redundancy Check (CRC) Checksum (4 bytes) fields in the Ethernet frame, resulting in a maximum of 9022 bytes or greater. The system shall also support a configurable MTU between 1280 bytes and 1540 bytes to ensure packets can transit type 1 encryptors. The system default MTU shall be 1540 bytes. The SUT met this requirement the vendor LoC.

(g) Ethernet services of the system shall allocate a unique Ethernet MAC address to each Ethernet interface associated with a VLAN, as per IEEE 802.1Q. The SUT met this requirement with testing which included assigning unique Ethernet MAC address to Ethernet interface associated with a VLAN.

(h) Ethernet services of the system shall support "Link Aggregation," as per IEEE 802.3ad or IEEE 802.1AX-2008, and use with the Link Aggregation Control Protocol. The SUT met this requirement with the vendor LoC and using LACP for the 10 Gb interfaces used during the test.

(i) Ethernet services of the system shall provide Link Layer Discovery Protocol (LLDP), as per IEEE 802.1AB. The SUTmet this requirement with testing and the vendor LoC.

(4) The UCR 2013, section 14.5, states the system shall provide Fibre Channel (FC) physical interfaces and FCP interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303. The SUT met this requirement with the vendor's LoC and testing.

(5) The UCR 2013, section 14.6 includes the Converged Network Adapter Interface requirements in the subparagraphs below.

(a) The system shall provide physical interfaces for FCoE services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA). The SUT met this requirement with the vendor's LoC and testing. Test included copying files from one DSC to another using the 10GbE FCoE interfaces.

(b) The system shall provide physical interfaces for Data Center Bridging [DCB, also known as Converged Enhanced Ethernet (CEE)] features, and functionality, per the standards depicted in Table 14.6-1, Physical Interfaces for Data Center Bridging. Although the SUT supports the DCB requirement, this optional requirement was not tested and therefore is not included in this certification.

(6) The UCR 2013, section 14.7 includes the IP Networking requirements in the subparagraphs below.

(a) The system shall meet the IPv6 requirements defined in Section 5.2.2, Mapping of RFCs to UC Profile Categories, for a simple server/network appliance. The SUT met the critical IPv6 requirements with the vendor's LoC with the exceptions listed in the subparagraphs below.

1. The SUT does not support the ability to configure the product to ignore Redirect messages. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.

2. The SUT does not support being configured to only accept Redirect messages from the same router as is currently being used for that destination. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact.

3. The system shall provide statically provisioned or dynamically adjusted large IP packet receive buffers for replication (mirroring) session traffic received on the Ethernet physical interfaces. The receive buffers may be statically provisioned or the operating system of the system may dynamically self-adjust the packet receive buffer size based on measurements of the E2E path bandwidth, Maximum Segment Size (MSS), Round Trip Time (RTT), and the percentage of packet loss. The system shall provide a default and minimum IP packet receive buffer size of 2048 KB per replication (mirroring) session. The system shall provide a statically provisioned or dynamically adjusting maximum IP packet receive buffer size of up to 8192 KB per replication (mirroring) session. The SUT does not support statically provisioning or dynamically adjusting large IP packet receive buffers for replication (mirroring) session traffic received on the Ethernet physical interfaces. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact with a condition of fielding. The SUT must connect to a routed subnet that utilizes IPv4 and IPv6 path MTU discovery and TCP MSS adjustment.

(b) The system shall provide an optimized congestion control (congestion avoidance) algorithm in Transmission Control Protocol (TCP) for avoidance of traffic loss on communications paths in high-speed networks with high latency or large bandwidth-delay products. The SUT met this requirement with the vendor's LoC.

(7) The UCR 2013, section 14.8 includes the Name Services requirements in the subparagraphs below.

(a) The system shall provide Lightweight Directory Access Protocol (LDAP) directory services per IETF RFC 4510. The SUT met this requirement with the vendor's LoC.

(b) The system shall provide Kerberos authentication service per IETF RFC 4120. The SUT does not support this requirement. The SUT met this requirement with the vendor's LoC.

(c) The system shall provide Domain Name System (DNS) client functionality. The SUT met this requirement with testing. The functionality was verified by finding a host name when entering an IP address and finding an IP address when entering a host name.

(d) The system shall provide DNS client-side Load Balancing. This requirement was met the vendor's LoC and additional documentation describing the method for DNS client-side load balancing.

(e) The system shall provide Network Information Service (NIS) client directory service functionality. Although the SUT supports the NIS requirement, this optional requirement was not tested because a NIS server was not available and therefore is not included in this certification. There is no operational impact of not testing NIS. The SUT uses DNS and Cisco's native discovery protocol for client-server directory services.

(f) The system shall provide NIS Netgroups client directory service functionality. This requirement is not applicable. Although the SUT supports the NIS server, this requirement was not tested because a NIS server was not available and therefore is not included in this certification. There is no operational impact of not testing NIS. The SUT provides DNS and Cisco's native discovery protocol for client-server directory services.

(g) The system shall provide Network Basic Input/Output System (NETBIOS) over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS). The SUT does not support this optional requirement. Although the SUT supports WINS, this optional requirement was not tested because a WINS server was not available and therefore is not included in this certification. There is no operational impact since the SUT provides DNS functionality. DNS has replaced WINS since Microsoft made changes to NetBIOS, allowing it to use the TCP/IP stack to perform its job (NetBIOS over TCP/IP) and most DNS servers are able to handle NetBIOS requests.

(h) The system shall provide Internet Storage Name Service (iSNS) client functionality per IETF RFC 4171. Although the SUT supports iSNS client functionality, this requirement was not tested because an iSNS server was not available for test and therefore is not included in this certification. There is no operational impact since the SUT was able to provide discovery, management and configuration of iSCSI and Fibre Channel devices on the TCP/IP network without the use of an iSNS server.

(i) If the system has a FC interface then the system shall provide FC Name and Zone Service. The SUT met this conditional requirement with testing. Testing included creating a zone with several members in one Virtual Storage Area Network (VSAN) allowing those members belonging to that zone to communicate. Next, a new zone was created within the same VSAN and a couple of members were moved from the original zone to the new zone. The members moved to the new zone were no longer able to communicate with the member in the original zone. In addition, access control for different VSAN was also verified. Members in one VSAN were not able to communicate with members in another VSAN.

(8) The UCR 2013, section 14.9 includes the Security Services requirements in the subparagraphs below.

(a) The system shall provide IPSec per RFC 4301. The SUT does not support this optional requirement and therefore is not included in this certification.

(b) The system shall provide Encapsulating Security Payload (ESP) per RFC 4303. The SUT does not support this optional requirement and therefore is not included in this certification.

(c) The system shall provide Internet Key Exchange version 2 (IKEv2) per RFC 4306. The SUT does not support this optional requirement and therefore is not included in this certification.

(d) The system shall provide a configurable Packet Filter (Firewall) service to block unauthorized access (for intrusion prevention) while permitting authorized communications. The Packet Filter service shall use a “stateless” design that does not degrade performance and shall filter all packets received based on interface, source IP address, protocol, port, Type of Service (TOS), or Time To Live (TTL). The Packet Filter service shall provide a configuration policy for defining combinations of multiple packet match rules and processing actions. The SUT met this requirement with the vendor’s LoC.

(e) The system shall provide encryption of data at rest at a minimum of AES-256 in accordance with Federal Information Processing Standard (FIPS) 140-2 level 1 or higher to provide the following capabilities:

1. Rapid crypto-shredding (destruction) of data, in accordance with National Institute of Standards and Technology 800-88, for tactical systems that operate in harm’s way and may fall into enemy hands. The met this requirement with the vendor’s LoC.

2. Rapid recovery from sensitive data spills, where the wrong data is accidentally written to the wrong place. The SUT met this requirement with the vendor’s LoC.

(f) The system shall comply with all appropriate STIGs to include the Database Security Technical Implementation Guide. Security testing is accomplished by a JITC-led Cyberseccurity test team and the results published in a separate report, Reference (e).

(9) The UCR 2013, section 14.10, states the system shall provide an Application Programming Interface (API) to enable interaction with other software and systems. The interactions shall include routines, data structures, object classes, and protocols used to

communicate between the consumer and implementer of the API. The API protocol and message format (e.g., Extensible Markup Language [XML]) shall be subject to the specific vendor system operating system implementation. The SUT met this requirement with the vendor's LoC.

(10) The UCR 2013, section 14.11 includes the Class of Service and Quality of Service requirements in the subparagraphs below.

(a) The system shall provide Class of Service (CoS) and Quality of Service (QoS) marking on egress traffic at layer 2 per IEEE 802.1p and, Section 7.2.1.3, Class of Service Markings, and Section 7.2.1.4, Virtual LAN Capabilities. Traffic classification and marking must occur before the egress transmission of the Ethernet frame with a rule or policy engine that matches on various storage and management protocol types as offered by the system. The SUT met this requirement with testing using a site provided APL network switch.

(b) The system shall provide CoS and QoS marking on egress traffic at layer 3 per Section 6, Network Infrastructure End-to-End Performance. Traffic classification and marking must occur before the egress transmission of the IP packet with a rule or policy engine that matches on various storage and management protocols that occur within the system, such as those listed in Table 14.11-1. The IP packets are marked in the TOS field of the IPv6 packet header with Differentiated Services Code Point (DSCP) values from 0 and 63, inclusive. These are to be used in the ASLAN, non-ASLAN, and extended networks for per-hop CoS and QoS traffic conditioning by the network elements. The SUT met this requirement with testing using a site provided APL network switch.

(11) The UCR 2013, section 14.12 includes the Virtualization requirements in the subparagraphs below. The SUT does not support the optional vDSC capabilities. Therefore, the requirements in the following subparagraphs do not apply and are not included in this certification. There is no impact of the SUT not supporting this optional requirement.

(a) The system shall provide virtualized Data Storage Controller (vDSC) functionality and individual protocol server processes. The vDSC shall meet all the requirements of a DSC with minor exceptions that are related to design and technical limitations associated with the complete virtualization of an operating system, which include internal counters for attributes of the physical system, QoS traffic processing, and per vDSC Mobile IP correspondent node binding cache limitations.

(b) The vDSC capability within the system shall provide secure, Private Networking Domains (PNDs) for Ethernet, VLANs, and IP that isolate the network domains of system units. The PND shall support the use of duplicate IP addresses and IP subnet address ranges among those of any other configured vDSC in the system. The PND shall provide a dedicated IP Forwarding Information Base (FIB) per vDSC.

(c) The vDSC shall provide an individual Command Line Interface (CLI) context with the full command set of the system, with the scope of the commands limited to the individual vDSC CLI context.

(d) The vDSC shall provide a programmatic API with the full command set of the system with the scope of the API commands limited to the individual vDSC context.

(e) The vDSC capability within the system shall provide an individual GNS unique from the system or shall provide a single name space that provides the capability to aggregate disparate hardware and storage architectures into a single file system. The GNS shall provide the capability to aggregate disparate and remote network-based file systems, providing a consolidated view to reduce complexities of localized file management and administration. The GNS shall provide large working pools of disks and transparent data migration, and shall serve to reduce the number of storage mount points and shares. The single name space shall be spread across multiple physical network access server heads all representing the same file system without replication. The single name space shall include the ability to tier data automatically within the same file system.

**c. Hardware/Software/Firmware Version Identification.** Table 3-3 provides the SUT components' hardware, software, and firmware tested. The JITC tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

**7. TESTING LIMITATIONS.** JITC test teams noted the following testing limitations including the impact they may have on the interpretation of the results and conclusions:

a. Although the SUT supports the NIS requirement, this optional requirement was not tested because a NIS server was not available and therefore is not included in this certification. There is no operational impact of not testing NIS. The SUT uses DNS and Cisco's version of LDAP for client-server directory services.

b. Although the SUT supports the NIS server, this requirement was not tested because a NIS server was not available and therefore is not included in this certification. There is no operational impact of not testing NIS. The SUT provides DNS and Cisco's version of LDAP for client-server directory services.

c. Although the SUT supports WINS, this optional requirement was not tested because a WINS server was not available and therefore is not included in this certification. There is no operational impact since the SUT provides DNS functionality. DNS has replaced WINS since Microsoft made changes to NetBIOS, allowing it to use the TCP/IP stack to perform its job (NetBIOS over TCP/IP) and most DNS servers are able to handle NetBIOS requests.

d. Although the SUT supports iSNS client functionality, this requirement was not tested because an iSNS server was not available and therefore is not included in this certification. There is no operational impact since the SUT was able to provide discovery, management and configuration of iSCSI and Fibre Channel devices on the TCP/IP network without the use of an iSNS server.

**8. CONCLUSION(S).** The SUT meets the critical interoperability requirements for a Data Storage Controller in accordance with the UCR and is certified for joint use with other UC Products listed on the Approved Products List (APL). The SUT meets the interoperability requirements for the interfaces listed in Table 3-1.

# DATA TABLES

## Table 3-1. SUT Interface Status

| Interface | Threshold CR/FR Requirements (See Note 1.) | Status | Remarks |
|---|---|---|---|
| **Network Attached Storage (NAS) Interfaces** | | | |
| 1 GbE (Ethernet) (R) | 1 | Not Met | See Note 2. |
| 10 GbE (Ethernet) (R) | 1 | Met | |
| **Storage Array Net (SAN) Interfaces** | | | |
| Fibre Channel (FC) | 1 | Met | |
| FC Protocol (FCP) | 1 | Met | |
| **Out-of-band Management Interfaces** | | | |
| 10 Mbps Ethernet (R) | 1 | Met | |
| 100 Mbps Ethernet (R) | 1 | Met | |
| 1 GbE Ethernet (R) | 1 | Met | |
| **Converged Network Adapter (CNA) Interfaces** | | | |
| 10 GbE (Ethernet) (R) | 1 | Met | |

**NOTE(S):**

1. The UCR does not identify interface CR/FR applicability. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column are cross-referenced with Table 3.
2. The SUT does not support 1 GbE NAS interfaces. DISA adjudicated this discrepancy as a change requirement with no operational impact.

**LEGEND:**

| | | | |
|---|---|---|---|
| CNA | Converged Network Adapter | NAS | Network Attached Storage |
| CR | Capability Requirement | R | Required |
| FR | Functional Requirement | SAN | Storage Array Net |
| GbE | Gigabit Ethernet | SUT | System Under Test |
| ID | Identification | UCR | Unified Capabilities Requirements |
| Mbps | Megabits per second | | |

## Table 3-2. Capability and Functional Requirements and Status

| CR/FR ID | UCR Requirement (High-Level) (See note 1.) | UCR 2013 Reference | Status |
|---|---|---|---|
| 1 | Data Storage Controller (DSC) (R) | | |
| | Storage System (R) | 14.2 | Met |
| | Storage Protocol (R) | 14.3 | Partially Met (See note 2.) |
| | Network Attached Storage Interface (R) | 14.4 | Met (See note 3.) |
| | Storage Array Network Interface (O) | 14.5 | Met |
| | Converged Network Adapter Interface (O) | 14.6 | Met |
| | IP Networking (R) | 14.7 | Partially Met (See note 4.) |
| | Name Services (R) | 14.8 | Met |
| | Security Services (R) | 14.9 | Met |
| | Interoperability (R) | 14.10 | Met |
| | Class of Service and Quality of Service (R) | 14.11 | Met |
| | Virtualization (O) | 14.12 | Not Tested (See note 5.) |

**NOTES:**

1. The annotation of ‘required’ refers to a high-level requirement category. The applicability of each sub-requirement is provided in Table 3-5.
2. The SUT does not support GNS/single name space requirement. DISA has accepted and approved the vendor’s POA&M and adjudicated this discrepancy as having a minor with a condition of fielding.
3. The SUT does not support the 1 GbE interface. DISA adjudicated this discrepancy as a change requirement.
4. The SUT does not support being configured to only accept Redirect messages from the same router as is currently being used for that destination. DISA has accepted and approved the vendor’s POA&M and adjudicated this discrepancy as having a minor operational impact.
5. The SUT does not support the optional vDSC requirements and therefore are not included in the certification.

## Table 3-2. Capability and Functional Requirements and Status (continued)

**LEGEND:**

| | | | |
|---|---|---|---|
| CR | Capability Requirement | PO&AM | Plan of Action and Milestones |
| DSC | Data Storage Controller | R | Required |
| DISA | Defense Information Systems Agency | SUT | System under Test |
| FR | Functional Requirement | UCR | Unified Capabilities Requirements |
| GNS | Global Name Space | v | Version |
| IP | Internet Protocol | vDSC | Virtualized Data Storage Controller |
| O | Optional | | |

## Table 3-3. SUT Hardware/Software/Firmware Version Identification

| Component (See notes 1 and 2.) | Release | Sub-component | Function |
|---|---|---|---|
| **FAS8040**, FAS2520, FAS2552, FAS2554, FAS2620 AFF A200, FAS2650, FAS8020, FAS8040, AFF8040, FAS8200, AFF A300, FAS8060, FAS8080 EX, AFF8080 EX, FAS9000, AFF 700, AFF A700s | ONTAP Release 9.1 | Not Applicable | Primary and Secondary Data Storage Controllerss |

**NOTES:**

1. Components bolded and underlined were tested by JITC. The other components in the family series were not tested, but are also certified for joint use. JITC certifies those additional components because they utilize the same software and similar hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes.
2. Expanded I/O products have a dual enclosure and 12 PCIe expansion slots instead of a single enclosure and 4 PCIe expansion slots.

**LEGEND:**

| | | | |
|---|---|---|---|
| AFF | All Flash FAS | JITC | Joint Interoperability Test Command |
| FAS | Fabric Attached Stroage | PCIe | Peripheral Component Interconnect Express |
| I/O | Input/Output | SUT | System Under Test |
| IOXM | I/O Expansion Module | | |

## Table 3-4. Test Infrastructure Hardware/Software/Firmware Version Identification

| System Name | Software Release | Function |
|---|---|---|
| **Required Ancillary Equipment** | | |
| Active Directory | | |
| Public Key Infrastructure | | |
| SysLog Server | | |
| **Test Network Components** | | |
| Cisco Nexus 5548UP (See note) | NX OS 6.0(2)N2(7) | Switch for Primary DSC and Secondary |
| Fujitsu RX300S7 Server (See note) | Windows Servers 20012 R2 Standard Service | Management Server |
| Fujitsu RX300S7 Server (See Note) | Red Hat Linux | NFS Client Server and SAN |
| Dell S4048 ON | 9.8(0.0P5) | Edge Switch |
| Brocade NetIron | 5.6.0aT183 | Edge Switch |
| Cisco 4506 | 15.0 (2) SG5 | Layer 3 Router |

**NOTE(S):** The components are site provided.

**LEGEND:**

| | | | |
|---|---|---|---|
| DSC | Data Storage Controller | SAN | Storage Area Network |
| NFS | Network File System | OS | Internetwork Operating System |
| NX | Nexus | | |